METHOD AND APPARATUS FOR DETECTING DENIAL-OF-SERVICE ATTACKS USING KERNEL EXECUTION PROFILES

ABSTRACT

One embodiment of the present invention provides a system that detects denial-of-service attacks by using an execution profile for a kernel of a server computer system. The system produces a run-time execution profile by gathering statistics related to execution of a protocol stack within the kernel, wherein the protocol stack processes packets received from client computer systems. Next, the system compares the run-time execution profile with a normal execution profile, wherein the normal execution profile is representative of execution when the server is not subject to a denial-of-service attack. If the run-time execution profile deviates from the normal execution profile, the system indicates that a denial-of-service attack is taking place.